高素质技术技能型人才培养教程

电子商务安全

俞国红　主编

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

高等职业教育产教融合系列教材·电子商务类

电子商务安全

主　编　俞国红
副主编　郑广成
参　编　潘启超

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 提 要

本书包含了电子商务安全概述、电子商务的网络安全技术、数据加解密技术、数字证书和数字签名技术、电子商务安全协议、电子支付安全、电子商务法律法规七个模块内容，较为系统地讲述电子商务面临的安全问题与安全控制要求、操作系统加固技术、数据加密技术、数据备份恢复技术、常见的计算机病毒及其防治方法。通过学习实际的电子商务安全项目，了解和掌握电子商务安全的专业知识，具备电子商务安全的实际工作技能，能够从事电子商务安全工程师岗位的工作。

本书涉及了电子商务安全研究领域的最新成果，具体包括电子商务数据备份技术、密码技术中的量子密码技术、电子商务安认证签名技术以及最新的电子商务安全法律法规等。

本书可作为高等院校电子商务专业、信息管理与信息系统专业、管理类专业、计算机类专业等相关本专科专业学生的教材。

图书在版编目（CIP）数据

电子商务安全/俞国红主编. —北京：北京理工大学出版社，2019.10（2019.11 重印）
ISBN 978-7-5682-7572-9

Ⅰ. ①电…　Ⅱ. ①俞…　Ⅲ. ①电子商务-安全技术-高等学校-教材　Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字（2019）第 204589 号

出版发行 / 北京理工大学出版社有限责任公司
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 / （010）68914775（总编室）
　　（010）82562903（教材售后服务热线）
　　（010）68948351（其他图书服务热线）
网　　址 / http：//www.bitpress.com.cn
经　　销 / 全国各地新华书店
印　　刷 / 唐山富达印务有限公司
开　　本 / 787 毫米×1092 毫米　1/16
印　　张 / 16　　责任编辑 / 钟　博
字　　数 / 379 千字　　文案编辑 / 钟　博
版　　次 / 2019 年 10 月第 1 版　2019 年 11 月第 2 次印刷　　责任校对 / 刘亚男
定　　价 / 45.00 元　　责任印制 / 施胜娟

前　言

本书讲述电子商务面临的安全问题与安全控制要求、加密技术在电子商务中的应用、常见的计算机病毒及其防治方法，通过实际的电子商务安全项目，使学生了解本专业的知识与技能，从而能够从事电子商务安全工程师岗位工作。

本书涉及电子商务安全最新研究领域，具体包括电子商务安全的备份技术、密码技术、认证技术以及电子商务安全法律法规等。本书培养学生具有电子商务安全的实际工作技能，具体的学习目标见下表。

学习内容	知识要求	能力要求	学时	
			理论	实践
模块一　电子商务安全概述	了解电子商务的风险与安全问题； 了解安全电子商务安全的要求； 了解电子商务安全保障体系	会制定安全保障的措施	2	2
模块二　电子商务的网络安全技术	熟悉互联网基本技术——TCP/IP 和 WWW 技术及其安全问题； 了解计算机网络中的身份认证技术和应用； 了解网络攻击方式和防御措施	会使用网络安全基本工具； 会使用虚拟机； 掌握防火墙技术； 会操作系统的安全配置； 掌握常见计算机病毒的防范技术	6	6
模块三　数据加解密技术	掌握密码学的基本概念	会使用工具破解常见密码； 会对文件进行加密	4	4
模块四　数字证书和数字签名技术	理解数字签名的概念、要求、原理和作用	会数字证书的申请和使用； 会信息加密和数字签名的操作； 能利用 PGP 软件实现数字签名	4	4
模块五　电子商务安全协议	了解电子商务安全协议标准； 了解 PKI 技术	会使用 PKI 技术进行数据加密和签名	4	4
模块六　电子支付安全	了解传统支付与电子支付的不同； 掌握网络支付与结算的整体理论与应用体系	能够在电子支付中注意安全保护	2	2

续表

学习内容	能力要求	知识要求	学时	
			理论	实践
模块七　电子商务法律法规	了解电子商务立法的概况；掌握《电子签名法》《电子商务法》的主要内容，了解电子合同与《合同法》的关系	能够利用数据电文法律知识分析案例； 会使用电子商务法律法规处理电子商务纠纷	2	2
合计			24	24

自 2019 年开始进行《电子商务安全》课程思政教育实践，在专业课教学中融入课程思政内容，《电子商务安全》课程教学目标，分解为知识目标、能力目标、素质目标三部分，知识和能力目标重点培养学生具有电子商务安全保密、数据信息安全等方面技能和素养，素质目标重点培养学生成为具有社会主义核心价值观、职业伦理、科学和工匠精神、团队精神的现代职业人。教材中在每个章节嵌入了课程思政内容的二维码。使用手机扫描二维码，可以获取到 20 个思政元素，包含 3 个电子支付安全案例、4 个科学故事、6 个数据安全运用实例，7 个法律法规知识。通过精心设计，课程思政的教学活动通过情境互动、体验互动、探究互动，将马克思主义理论教育、中国梦教育、社会主义核心价值观教育、道德修养教育、法治教育五大类思政元素融入专业课程教学之中，实现课程思政教育与专业知识技能教育的有机统一，坚持立德树人这一根本任务，贯彻落实课程思政育人目标。

本书的学习资源丰富，在部分章节中安排了知识链接的二维码，读者可以使用手机扫描，通过移动阅读方式浏览知识点对应的技术文章、新闻、视频等学习资源。本书的学习资料共 70 个，其中技术文章 30 篇、教学使用的 PPT 32 个、微课视频 8 个，读者可进入《电子商务安全》课程在超星泛雅在线教学平台（网址：http：//mooc1. chaoxing. com/course/95855199. html）下载。

本书由俞国红、郑广成和企业工程师潘启超共同编写完成。本书得到江苏“青蓝工程”项目资助。由于作者水平有限书中难免有不当和错误之处，请读者将阅读过程中发现的问题发送到 E－mail：wuygh@126. com。

编　者

目　录

模块一

电子商务安全概述

电子商务经济以其开放性、全球化、低成本、高效率的优势，广泛渗透到生产、流通、消费及民生等领域，在培育新业态、创造新需求、拓展新市场、促进传统产业转型升级、推动公共服务创新等方面的作用日渐凸显，成为国民经济和社会发展的新动力，是推动“互联网 +”发展的重要力量，是新经济的主要组成部分。

互联网是一个庞大的信息和数据来源，电子商务是利用 Internet 进行的交易活动。中国电子商务研究中心统计数据显示，截至 2018 年 12 月，中国电商服务企业从业人员超过 410 万人，根据中国互联网络信息中心（China Internet Network Information Center，CNNIC）发布的《中国互联网络发展状况统计报告》，在电子商务方面，52.26% 的用户最关心的是交易的安全可靠性。在我国，电子商务交易中的信用卡盗用、信息资料丢失等现象时有发生。电子商务安全面临诸多问题，主要涉及如下 4 个方面：

（1）保密性：保证大量保密信息在公开网络的传输过程中不被窃取；

（2）完整性：保证所传输的信息不被中途篡改及通过重复发送被伪造；

（3）身份认证与授权：对通信双方进行认证，以保证双方身份的正确性；

（4）抗抵赖：保证电子商务活动任何一方对已发生操作的不可否认性。

造成电子商务安全问题的原因主要有四个：信息泄露、信息篡改、身份识别、信息破坏，如图 1 – 1 所示。

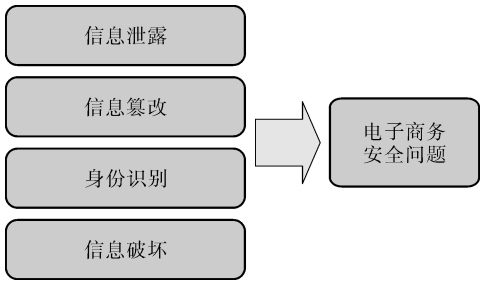

图 1 – 1　电子商务安全问题的原因

信息泄露：对个人信息缺乏正确的保护意识，加上系统存在技术漏洞，可导致用户个人信息、银行卡信息等的泄露。泄露的信息包括用户姓名、身份证号、银行卡类别、银行卡卡号、银行卡 CVV 码（卡号、有效期和服务约束代码生成的 3 位或 4 位数字）等。

信息篡改：攻击者窃取电子商务网站的数据库，获得想要的信息，甚至篡改、删除对网

站至关重要的信息，破坏数据的准确性和完整性。

身份识别：电子身份认证能够利用简单的身份载体，识别用户的数字身份，保证操作者的物理身份与数字身份相对应，目的是确保系统安全运行和通信的保密和安全。

信息破坏：数据因被非授权地进行增删、修改或破坏而受到损失，信息的完整性遭到破坏。

项目 1.1　认识电子商务安全

电子商务安全从字面上可以拆分为“电子商务”“安全”两个词。电子商务安全主要分为 2 个方面：计算机网络安全和商务交易安全。其中，计算机网络安全包括计算机网络硬件的安全与计算机网络软件的安全；由于 Internet 存在很多安全隐患，这给电子商务的交易带来了安全威胁。电子商务安全的知识脉络如图 1－2 所示。

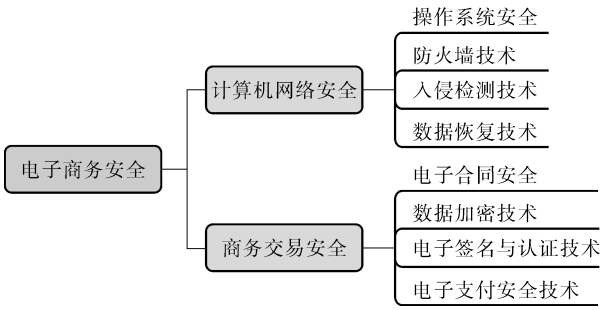

图 1－2　电子商务安全的知识脉络

任务 1　认识电子商务安全


思政元素 1


思政元素 2

【任务描述】

雅鹿公司电子商务部的小王从事电子商务部的安全专员工作。电子商务部总监要求小王了解国内电子商务安全的现状，并重点使用百度搜索引擎查找相关信息。

【任务分析】

了解电子商务安全隐患和威胁、电子商务安全隐患的防范措施；理解电子商务安全的中心内容；掌握电子商务安全体系的具体内容。

【知识准备】

1. 电子商务安全的概念

电子商务安全就是保护电子商务系统里物理化和电子化的资产，防止未经授权的访问、使用、篡改或破坏。电子商务安全的中心内容是为用户提供稳定的服务，保证商务数据的完整性。

2. 电子商务安全技术的概念

电子商务系统中使用的安全技术包括网络安全技术、信息加密技术、数字签名技术、密钥管理技术、安全认证技术、防火墙技术以及相关的安全协议标准等。电子商务安全技术的组成如图 1－3 所示。

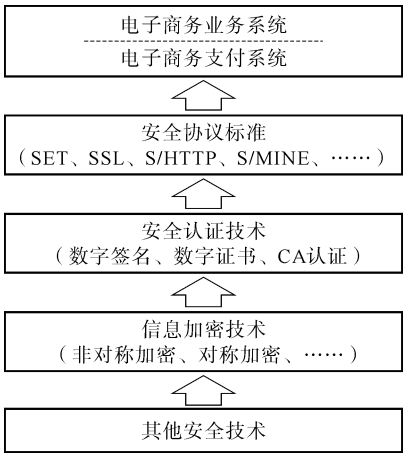

图 1－3　电子商务安全技术的组成

【任务实现】

1. 电子商务安全面临的严峻形势

1）电子商务安全体系结构不完整

电子商务是在开放的互联网上进行的贸易，大量的商务信息在计算机上存放和传输，其系统属于一个中央系统，把服务提供商以及客户、银行有效地联系在一起。目前，电子商务信息传输、交易信用、平台管理、法律规范等方面的安全防护体系还不健全。

利用电子商务安全体系结构来解决电子商务系统的安全问题，目前电子商务安全体系由下至上分别是安全协议层、安全认证层、加密技术层、网络安全层四层。电子商务系统面对日益复杂的安全问题，需要电子商务安全体系结构不断完善功能，为电子商务活动保驾护航。

2）电子商务管理体制不健全

目前虽然我国政府已将电子商务的管理提上日程，逐渐建立并制定了有关的电子商务法规和政策，为我国电子商务的发展提供了基本的法律保障，但某些方面仍不成熟。例如，如何引入电子签名、数字签名等管理方式保障信息的安全？在交易过程中，如何明确双方的责任？如何保障信息不泄露？这些方面都有待进一步加强和完善。

3）电子商务安全产品不过硬

目前市场上有关电子商务安全的产品数量不少，但真正通过国际和国家安全认证的却相当少。另外，拥有自主知识产权的安全技术和产品很少。目前构成我国信息基础设施的网络、硬件、软件等产品几乎都建立在以美国为首的少数几个发达国家的核心信息技术之上。中兴公司芯片事件再一次提醒我们，高新技术产品要有创新，才能有话语权。

4）多种威胁交织，频繁出现

电子商务安全面临的安全威胁主要来源于以下 3 个方面：

（1）非人为、自然力造成的数据丢失、设备失效、线路阻断。

（2）人为但属于操作人员无意的失误造成的数据丢失。

（3）来自外部和内部的恶意攻击和入侵。这种因素是当前电子商务安全所面临的最大威胁，极大地影响了电子商务的顺利发展。

电子商务安全的威胁如图 1－4 所示。

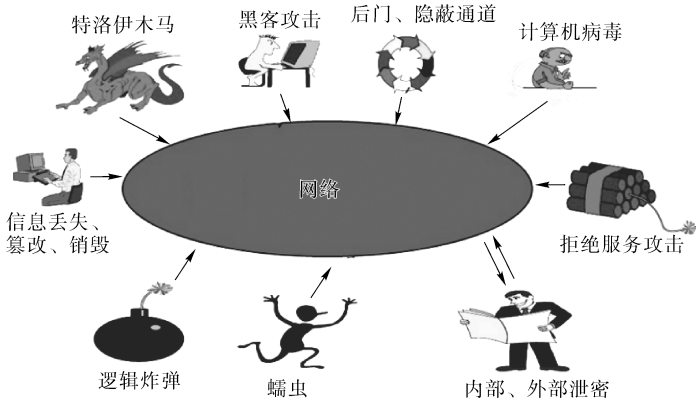

图 1－4　电子商务安全的威胁

上述安全威胁，根据针对电子商务系统的攻击手段，可归纳为以下几种：

（1）中断：采取破坏硬件、线路或文件系统等方式，阻断用户访问，攻击系统的可用性。

（2）窃取：采取搭线、电磁窃取和分析业务流量等方式获取有用信息，攻击系统的机密性。

（3）篡改：结合其他手段修改秘密文件或核心内容，攻击内容的完整性。

（4）伪造：伪造假身份接入系统，假冒合法人接入系统，破坏消息的接收和发送，攻击系统的真实性。

（5）恶意攻击：采取施放电子邮件炸弹等方式，攻击系统的健壮性和容载能力。

黑客攻击方式如图 1－5 所示。

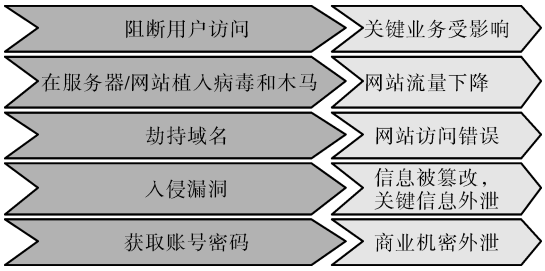

图 1－5　黑客攻击方式

2. 电子商务安全基础知识

电子商务安全分为实体安全（又称物理安全）、运行安全、信息安全。其结构如图 1－6 所示。

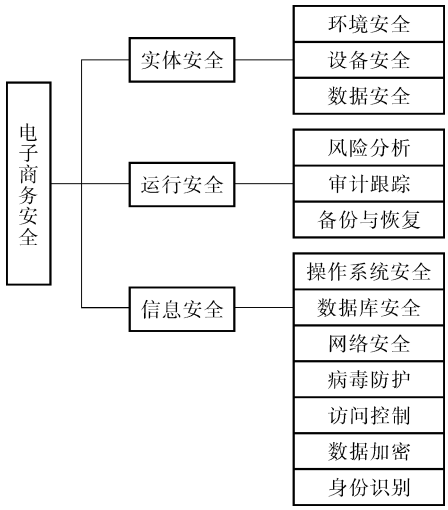

图 1－6　电子商务安全的结构

1）实体安全

实体安全是保护计算机设备、设施及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施、过程。实体安全是电子商务安全的最基本保障，是整个安全系统不可缺少的组成部分。

（1）实体安全的主要内容。

①环境安全：主要是对电子商务系统所在的环境实施安全保护，如区域保护和灾难保护。

②设备安全：对电子商务系统的设备进行安全保护，主要包括设备的防盗、防毁、防电磁信息辐射泄露、防止线路截获、抗电磁干扰及进行电源保护等。

③数据安全：电子商务系统中存放着大量机密敏感的数据，这些数据是电子商务企业运营时的重要信息。数据安全是指对电子商务数据实施安全存储、安全删除和安全销毁，防止数据被非法复制。

（2）实体安全的常见不安全因素。

①自然灾害（如地震、火灾、水灾等）、物理损坏（如硬盘损坏、设备使用寿命到期、外力致损等）、设备故障（如停电断电、电磁干扰等）。

a. 特点：突发性、自然性、非针对性。

b. 破坏性：对电子商务信息的完整性和可用性威胁最大。

c. 解决方法：采取各种防护措施，随时备份数据等。

②电磁辐射（监听微机操作过程）、乘虚而入（如合法用户进入安全进程之后半途离开）、痕迹泄露（如密码、密钥等保管不善，被非法用户获得）等。

a. 特点：隐蔽性、人为实施的故意性、信息的无意泄露性。

b. 破坏性：破坏电子商务信息的保密性。

c. 解决方法：采取辐射防护、设置密码、隐藏销毁等手段。

③操作失误（如偶然删除文件、格式化硬盘、拆毁线路等）、意外疏漏（如系统掉电、“死机”等）。

a. 特点：人为实施的无意性、非针对性。

b. 破坏性：破坏电子商务信息的完整性和可用性。

c. 解决方法：状态检测、报警确认、应急恢复等。

（3）防止信息在空间上扩散的措施。

①对机房及重要信息的存储、收发部门进行屏蔽处理。

②对本地网、局域网传输线路传导辐射进行抑制。

③对终端设备辐射进行防范。

④一般采取的措施：订购设备时应选取低辐射产品；采取主动式的干扰设备，用干扰机破坏窃取信息的行为。

2）运行安全

运行安全即为保障系统功能的安全实现，提供一套安全措施来保护信息处理过程的安全。其主要由 3 个部分组成：风险分析、审计跟踪、备份与恢复。

（1）风险分析。其是指对系统进行动态分析、测试、跟踪并记录系统的运行，以发现系统运行期的安全漏洞；对系统进行静态分析，以发现系统潜在的威胁，并对系统的脆弱性作出分析。

（2）审计跟踪。其是指记录和跟踪系统各种状态的变化，保存、维护和管理审计日志，如记录对系统故意入侵的行为。

（3）备份与恢复。其是指对系统设备和系统数据的备份和恢复；在紧急事件或安全事故发生时，提供保障电磁系统继续运行或紧急恢复所需要的策略。

3）信息安全

信息安全即指防止信息被故意的或偶然的非授权泄露、更改、破坏或使信息被非法的系统辨识、控制，也就是要确保信息的完整性、保密性、可用性和可控性。

信息安全主要由 7 部分组成：操作系统安全、数据库安全、网络安全、病毒防护、访问控制、数据加密和身份识别。

3. 电子商务活动中的安全隐患

在电子商务活动中，主要存在以下几种安全隐患：

（1）信息在网络传输过程中被截获。攻击者可能通过互联网、公共电话网，以搭线或在电磁波辐射范围内安装截收装置等方式，截获传输的机密信息，或通过对信息流量、流向、通信频率和长度等参数的分析，推断出有用信息、如消费者的银行账号、密码等。

（2）传输的文件被篡改。攻击者可能从三方面破坏信息的完整性，如表 1－1 所示。

表 1－1　破坏信息完整性的攻击方法

攻击方法	破坏信息的完整性
篡改	改变信息流的次序，更改信息的内容，如购买商品的出货地址
删除	删除某个消息或消息的某些部分
插入	在消息中插入一些信息，让收方读不懂或接收错误的信息

（3）假冒他人身份。冒充他人身份包括冒充领导发布命令、调阅文件；冒充他人消费，

栽赃；冒充主机欺骗合法主机及合法用户；冒充网络控制程序，套取或修改使用权限、密钥等信息；接管合法用户，欺骗系统，占用合法用户的资源。

（4）伪造电子邮件。伪造电子邮件包括虚开网站和商店，给用户发电子邮件，收购货单；伪造大量用户，发电子邮件，穷尽商家资源，使合法用户不能正常访问网络资源，使有严格时间要求的服务不能及时得到响应；伪造用户，发大量的电子邮件，窃取商家的商品信息和用户信用等信息。

（5）抵赖行为。抵赖行为包括发送信息者事后否认曾经发送过某内容；收到信息者事后否认曾经收到过某消息或内容；购买者发出订货单后不承认；商家卖出的商品后因价格不满意而不承认原有的交易。

4. 电子商务安全理念

电子商务安全是一个系统概念，不仅是技术性问题，也是管理性问题，其具体技术和管理方面的内容如图 1－7 所示。

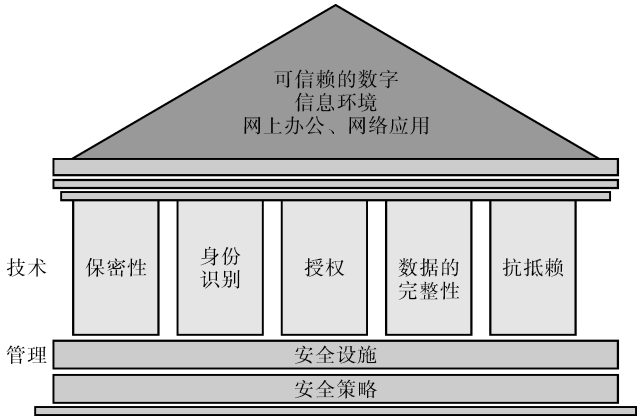

图 1－7　电子商务安全在技术和管理方面的内容

1）电子商务安全重在管理

近几年电子商务安全案例分析表明：电子商务企业缺乏针对内部人员的系统安全管理体制，是导致网络交易过程中信息泄密的主要原因。电子商务安全问题，与法律、道德和人的因素紧密地联系在一起，只有全面协调地发展，才能建立一个安全的电子商务系统。

2）电子商务安全重在防范

电子商务安全是相对的，没有一劳永逸的安全技术。电子商务安全是发展的、动态的。安全技术具有很强的敏感性、竞争性和对抗性，需要不断地检查、评估和调整相应的安全策略。

5. 电子商务安全的发展趋势

电子商务安全正在由目前的信息交易等单一环节、线上与线下结合的模式向集成电子认证、在线交易、在线支付、物流和信用服务一体化的方向发展，呈现出全程电子商务安全的发展态势。

【动手做一做】

在搜索引擎中，搜索以下关于电子商务安全的关键词，并对相关知识加以整理：主动攻

击、被动攻击、SSH、SSL、VNP、PKI、IDS、IPS、网络钓鱼、信息安全特征。

任务 2　了解电子商务安全需求

由于电子商务是在开放的互联网上进行的贸易，大量的商务信息在互联网上存放和传输，从而形成信息传输、交易信用、法律等方面的各种风险。电子商务安全需求主要包括数据传输的安全性需求、数据的完整性需求、身份验证需求、交易的不可抵赖性需求，以保证贸易数据的有效性。

【任务描述】

为了加深对电子商务安全威胁及其重要性的理解，雅鹿公司电子商务部总监要求小王了解电子商务安全的措施及相关技术。具体要求如下：

（1）上网搜集电子商务安全威胁的案例，要求搜集的案例不少于 3 个；

（2）分析电子商务安全的协议及措施；

（3）了解不同类型电子商务网站所采取的电子商务安全措施和技术。

请帮助小王完成上述任务。

【任务分析】

了解电子商务安全需求。

【任务实施】

1. 互联网安全防范措施的调查

阅读 CNNIC 最新的《中国互联网络发展状况统计报告》中关于电子商务安全和支付方面的数据及分析，了解中国电子商务发展的现状，并写一份 500 字的报告。

（1）进入中国互联网络信息中心网站：www. cnnic. cn。

（2）单击页面右下方“中国互联网络发展状况统计报告”链接。

（3）下载最新的《中国互联网络发展状况统计报告》。

（4）查找并比较其中关于电子商务安全和支付方面的数据，分析其变化的原因，形成并提交报告。

另外，某同学通过网上用户就“电子商务系统中采取什么安全措施”的小调查，得到如下调查数据：

密码加密：36. 9%；

防病毒软件：74. 5%；

防火墙：67. 6%；

电子签名：7. 3%；

不清楚，由系统管理员负责：7. 4%；

什么措施都不采用：3. 6%。

【讨论】从上述调查数据分析中能得到什么结论？

2. 电子商务安全隐患

1）电子商务交易平台的安全隐患

电子商务交易平台主要由电子商务服务器、电子商务软件/网站系统、电子商务数据库、

电子商务支付系统等组成。电子商务交易平台是整个电子商务安全的基础，但各种原因往往导致平台本身的不安全。

国内外的电子商务网站都发生过被黑客入侵的事件，例如，浙江义乌小商品批发网站曾经遭到黑客将近一个月的轮番攻击，网站图片几乎都不能显示，每天流失订单金额达上百万元。再如，阿里巴巴网站也曾确认受到不明身份的网络黑客攻击，这些黑客采取多种手段攻击了阿里巴巴在我国和美国的服务器，企图破坏阿里巴巴全球速卖通平台的正常运营。

近些年随着云计算和大数据存储的快速发展，数据存储的安全性受到了更加严峻的考验，面对海量数据，传统的安全防护措施显得苍白无力。

2）电子商务支付的安全隐患

传统的买卖双方是面对面的，因此较容易保证交易过程的安全性和建立起信任关系。但在电子商务过程中，买卖双方是通过网络联系的，由于距离的限制，建立交易双方的安全和信任关系存在一定难度。

由于电子商务交易双方往往无须见面，交易安全便显得重要。电子商务交易主体的身份是否真实？交易各方的通信是否安全？交易的结果是否具有效力？这些都是安全交易必须面对的问题。电子商务支付系统是电子商务活动的核心部分，近年来免密盗刷、电信网络诈骗等支付安全事件频发。例如，不断有不法分子利用钓鱼网站，伪装成支付页面，导致大量网络用户受骗，财产在不经意间被人骗走。

3. 电子商务的主要安全需求

电子商务交易双方（销售者和消费者）都面临安全威胁。电子商务的安全需求主要体现在以下几个方面。

1）信息有效性需求

电子商务以电子形式取代了纸张，如何保证这种电子形式的贸易信息的有效性和真实性是开展电子商务的前提。电子商务作为贸易的一种形式，其信息的有效性和真实性将直接关系到个人、企业和国家的经济利益和声誉。

2）信息机密性需求

电子商务作为贸易的一种手段，其信息直接代表着个人、企业和国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务是建立在一个较为开放的网络环境上的，商业防泄密是电子商务全面推广的重要保障。

3）信息完整性需求

电子商务简化了贸易过程，减少了人为干预，同时也带来维护商业信息的完整、统一的问题。数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中的信息丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。因此，电子商务系统应充分保证数据传输、存储及完整性检查的正确和可靠。

4）信息可靠性需求

可靠性要求即能保证合法用户对信息和资源的使用不会被不正当地拒绝；不可否认要求即能建立有效的责任机制，防止实体否认其行为；可控性要求即能控制使用资源的人或实体的使用方式。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写